Nortel Mobile Communication 3100 Series Portfolio

Nortel Mobile Communication Gateway 3100 Installation and Upgrades

Release: 2.1
Document Revision: 02.03

www.nortel.com

NN42030-300

Nortel Mobile Communication 3100 Series Portfolio
Release: 2.1
Publication: NN42030-300
Document status: Standard
Document release date: 9 May 2008

Sourced in Canada

LEGAL NOTICE

This document contains Nortel confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without Nortel’s express written authorization. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

Postinstallation 27

System software maintenance 45

Appendix A Port numbers and protocols 57

Appendix B Self-signed certificate generation 59

Index 61

Procedures

New in this release

This section details what’s new in *Nortel Mobile Communication Gateway 3100 Installation and Upgrades (NN42030-300)* for Nortel Mobile Communication 3100 (MC 3100) Release 2.1.

Features

This section describes the features that impact the book.

This release provides support for the new client, the Nortel Mobile Communication Client (MCC) 3100 for Windows Mobile Single Mode. The Mobile Communication Gateway 3100 supports the MCC 3100 for Windows Mobile Single Mode (unlike the MCC 3100 for Windows Mobile Dual Mode which does not interact with the MCG 3100).

MCG 3100 supports two methods to access the web console: Hypertext Transport Protocol (HTTP) and Secure HTTP (HTTPS).

Other changes

This document has been renamed from *Nortel Mobile Communication Gateway 3100 Installation* to *Nortel Mobile Communication Gateway 3100 Installation and Upgrades*.

The following changes were made to the document for MC 3100 Release 2.1

- streamlined the How to get help chapter and Introduction chapter
- remove references to specific communication servers, where possible
- Service update (SU) functionality added

Revision history

May 2008	Standard 02.03. This document is issued to support Nortel Mobile Communication 3100 Release 2.1. Only the release date changed.
April 2008	Standard 02.02. This document is issued to support Nortel Mobile Communication 3100 Release 2.1. Added the DNS port to Table 6 "Port usage" (page 57).
April 2008	Standard 02.01. This document is issued to support Nortel Mobile Communication 3100 Release 2.1.
December 2007	Standard 01.04. This document is up-issued to include changes in technical content documented in CR Q01788812.
October 2007	Standard 01.03. This document is up-issued to include changes in technical content for software installation and root certificates.
October 2007	Standard 01.02. This document is up-issued to include changes in technical content for MCG 3100 configuration parameter fields.
September 2007	Standard 01.01. This document is issued to support the Nortel Mobile Communications 3100 Series Portfolio Release 2.0 on Nortel Communication Server 1000 Release 5.0 and Nortel Multimedia Communication Server 5100 Release 4.0.

How to get help

This chapter explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation is current at the time the product is released. To check for updates to the latest documentation for the Nortel Mobile Communication 3100 Series Portfolio, go to http://www.nortel.com and navigate to the Technical Documentation page for Mobile Communication 3100.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:
http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835). Outside North America, go to the following Web site to obtain the telephone number for your region:
http://www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:
http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introduction

This chapter contains the following topics:

Subject

This document describes the Nortel Mobile Communication Gateway 3100 (MCG 3100) server installation, which is part of the Nortel Mobile Communication 3100 Series Portfolio.

Intended audience

This document is intended for network administrators and those involved in systems planning. Knowledge of telecommunications and IP telephony networks is required.

Conventions

The following sections describe the conventions used in this document.

Text conventions

Table 1 "Text conventions" (page 11) describes the text conventions in this document.

Table 1
Text conventions

Convention	Description
Bold text	Indicates a user interface object, for example a menu choice or screen name, for example: Press the **OK** soft key.

Table 1
Text conventions (cont'd.)

Convention	Description
Italic text	Indicates document titles, for example: See the *Mobile Communication Client 3100 for Windows Mobile User Guide (NN42030-100)*.
`CLI command text`	Indicates CLI command prompts, input, and output, for example: **`REQ NEW <zone #>`**.

Terminology

This document refers to the supported communication servers generically as *communication server*. For information on the supported communication servers, see the product bulletin at www.nortel.com.

Related information

This section lists information sources that relate to this document.

- *Nortel Mobile Communication Client 3100 for Blackberry User Guide (NN42030-101)*
- *Nortel Mobile Communication Client 3100 for Nokia User Guide (NN42030-102)*
- *Nortel Mobile Communication Client 3100 for Blackberry Quick Reference (NN42030-105)*
- *Nortel Mobile Communication Client 3100 for Nokia Quick Reference (NN42030-106)*
- *Nortel Mobile Communication Client 3100 for Windows Mobile Single Mode User Guide (NN42030-107)*
- *Nortel Mobile Communication Client 3100 for Windows Mobile Single Mode Quick Reference (NN42030-108)*
- *Nortel Mobile Communication 3100 Series — Planning and Engineering (NN42030-200)*
- *Nortel Mobile Communication Gateway 3100 — Administration (NN42030-600)*
- *Nortel Mobile Communication Client 3100 for Windows Mobile Dual Mode — Administration (NN42030-601)*
- *Nortel Mobile Communication Gateway 3100 Release Notes (NN42030-403)*

NTPs

The following NTPs are referenced in this document:

- *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*
- *Nortel Mobile Communication 3100 Series — Planning and Engineering (NN42030-200)*
- *Nortel Mobile Communication Gateway 3100 — Administration (NN42030-600)*

Fundamentals

This chapter contains the following topics:

Overview

This section describes the Nortel Mobile Communication Gateway 3100 (MCG 3100) server hardware and software components and provides an overview of the installation options.

The MCG 3100 supports the following clients:

- Nortel Mobile Communication Client 3100 (MCC 3100) for BlackBerry
- Nortel Mobile Communication Client 3100 for Nokia
- Nortel Mobile Communication Client 3100 for Windows Mobile Single Mode

This document refers to the supported clients using the generic term *clients*.

ATTENTION
The MCG 3100 does not support the MCC 3100 for Windows Mobile Dual Mode. The MCC 3100 for Windows Mobile Dual Mode communicates directly with the communication server.

MCG 3100 server components

Nortel supports the MCG 3100 server software installed only on the Nortel Linux Base, which is provided by Nortel.

ATTENTION
You must install the MCG 3100 software on a dedicated server that runs no other applications.

Hardware components

The MCG 3100 server runs only on the following supported commercial off-the-shelf (COTS) hardware:

- HP DL320G4 (NTDU97AAE5)
- IBM x306m (NTDU99AAE5)

Table 2 "Hardware requirements" (page 16) describes the supported hardware requirements.

Table 2
Hardware requirements

Hardware	Specification
Processor	3.0 GHz
Memory	2 GB DRAM
Hard Disk Drive	1-80 GB SATA Disk
Network Interface Card	2 1-GB Ethernet Cards
Power Supply	1 power supply

Software components

The MCG 3100 software installation includes the following software components:

- Mobile Communication Gateway (MCG) 3100—enables the clients to access advanced collaborative IP telephony services on the enterprise network. Using the clients, users can search the corporate directory, manage voice mail, dial by extension number, and hold group calls with predefined groups of users.
- MCG 3100 Administration Server—includes the Web Console, a Web-based tool that administrators use to start, stop, and reload server processes, update operating parameters, monitor users, track messaging statistics, and manage the distribution of client software. The Administration server also includes a database of server activity.
- MCG 3100 Group Call Server—hosts ad hoc conference calls with predefined groups of users within the enterprise network. The Group Call server includes a database of group call activities.

Installation options

Two installation options exist:

- MCG 3100 Server is installed on one server—all software components are installed on one supported COTS server. This is the nonredundant configuration.
- MCG 3100 Server is installed on two servers—all software components are installed on two supported COTS servers, configured identically. If one server fails or is unavailable, the clients switch to the other server. This is the redundant configuration.

For more information about these options, see “Nonredundant and redundant server implementations” (page 23).

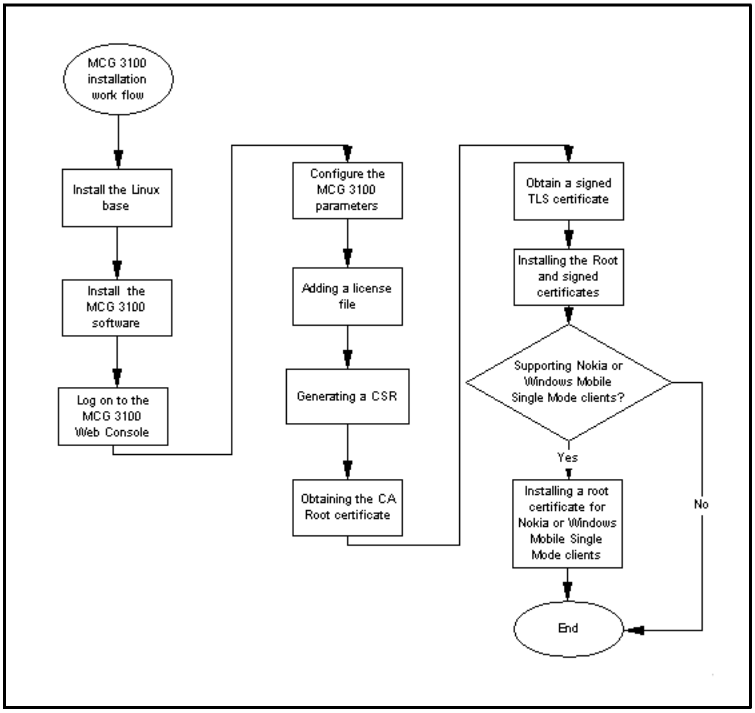
For a list of supported COTS servers, see “Hardware components” (page 16).

For more information about MCG 3100 redundant servers, see *Nortel Mobile Communication Gateway 3100 — Administration (NN42030-600)*.

Overview of the MC 3100 installation

Figure 1 "Installation overview" (page 17) shows the task flow for the MCG 3100 installation.

Figure 1
Installation overview


MCG 3100 installation work flow
Install the Linux base
Install the MCG 3100 software
Log on to the MCG 3100 Web Console
Configure the MCG 3100 parameters
Adding a license file
Generating a CSR
Obtaining the CA Root certificate
Obtain a signed TLS certificate
Installing the Root and signed certificates
Supporting Nokia or Windows Mobile Single Mode clients?
Yes
No
Installing a root certificate for Nokia or Windows Mobile Single Mode clients
End

Before you start the installation, read *Nortel Mobile Communication 3100 Series — Planning and Engineering (NN42030-200)*.

Preinstallation

This chapter contains the following topics:

Overview

Before you install the Mobile Communication Gateway 3100 (MCG 3100) server software, you must perform some preinstallation configuration and verification. To preconfigure the host server and the network enterprise network, perform the following tasks:

- Install the Nortel Linux operating system (OS) on the host server.
- Verify the enterprise network setup—the Lightweight Directory Access Protocol (LDAP) servers and Domain Name Server (DNS) must be installed and started.

Linux base installation

MCG 3100 uses the same Linux base as Nortel Communication Server (CS) 1000. However, during the Linux base installation for MCG 3100, you make the following platform-specific configuration changes:

- Physical connection
  Use only the eth1 physical network interface.

> **ATTENTION**
> Carefully observe the labels for the network interfaces of the specific platforms.
>
> — HP COTS platform: The network interfaces can be labelled (0,1) or (1, 2).
> The lower number is eth0 and the higher number is eth1.
>
> — IBM 306M platform: The network interfaces are labelled backwards. Interfaces (0, 1) are eth1 and eth0 respectively.

- IP addresses
  During the Linux base installation, the software prompts you to enter the TLAN and ELAN network interface IP addresses.

  — Configure the ELAN network interface IP with an unused private IP address.
  The IP standard reserves specific address ranges within Class A, Class B, and Class C for use by private networks (intranets). Table 3 "Reserved IP address ranges" (page 20) lists the reserved ranges of the IP address space.

  Table 3
  Reserved IP address ranges

Class	Private starting address	Private ending address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

  — Configure the TLAN network interface IP to the same IP address as the MCG 3100 and corresponding physical eth1 network interface.

To familiarize yourself with the Linux base installation procedure, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

Enterprise network verification

The following requisites must be installed and configured on the enterprise network:

- Domain Name Server (DNS)

  > **ATTENTION**
  > Nortel recommends that you program the DNS with the IP addresses of the License Server, the primary Enterprise Communication Server (ECS), and the alternate ECS.

  To verify that DNS is functional, use the ping command and enter the fully qualified domain name (FQDN) of a server on the network.

- Lightweight Directory Access Protocol (LDAP) server

To verify communication with the LDAP server, use the ping command. After the installation and commissioning is complete, you can verify that LDAP is working by performing a Corporate Directory (Corp Dir) search from a client.

You should ensure that the DNS and LDAP server can be accessed from the MCG 3100.

Supported LDAP servers

You can configure the MCG 3100 server to query a corporate directory so that the mobile clients can use the Directory lookup feature on their devices.

The Directory lookup feature uses LDAP to perform the query on one of the following supported directory servers:

- Active Directory/Exchange Server 2000 or 2003
- Nortel Common Network Directory (CND)
  Telephony Manager (TM) 3.1 in CS 1000 includes CND.

For information about configuring LDAP parameters on the MCG 3100, see *Nortel Mobile Communication Gateway 3100 — Administration (NN42030-600)*.

Installation

This chapter contains the following topics:

Overview

After you complete the preinstallation tasks, you install the Nortel Mobile Communication Gateway 3100 (MCG 3100) software in a nonredundant or redundant server implementation. During the MCG 3100 software installation, a number of prompts appear. You can accept the default value, or enter a new value at each prompt.

Nonredundant and redundant server implementations

For a nonredundant server implementation, install the software on a standalone server. For a redundant server implementation, install the software on two servers.

ATTENTION
You must install the license file on each of the servers in a redundant implementation.

Nonredundant server option

A nonredundant (or standalone) server implementation does not provide redundancy and therefore provides no failover protection. If a server component fails or becomes inaccessible, the mobile clients are denied access until the server recovers.

Redundant server option

A redundant server implementation provides high availability. If an active server component fails or becomes inaccessible, the mobile clients can restart a communication session with the backup server.

Rules for redundant server implementations

In a redundant server configuration, mobile clients access the active server, and not the inactive backup server. The two servers switch roles freely, and the following rules determine the status—either ACTIVE or INACTIVE:

- If you do not enter a backup IP address in the MCG 3100 Web Console, the server starts in ACTIVE mode.
- If you enter a backup IP address in the MCG 3100 Web Console, the server starts in STANDBY mode and attempts to locate the backup server.
- If the backup server is found in STANDBY mode, the server with the lower IP address is declared ACTIVE.
- If the backup server is found in ACTIVE mode, the backup server remains ACTIVE.
- If the backup server is not found within approximately 45 seconds, the local server is declared ACTIVE.
- If the ACTIVE server stops, the STANDBY server becomes ACTIVE after approximately 45 seconds.

> **ATTENTION**
> If the MCG 3100 server fails, the Administration Server and Group Call Server fail also.

Software installation

Install the MCG 3100 software after you complete the preinstallation configuration. For more information, see "Preinstallation" (page 19).

During the software installation, a number of prompts appear. You can either accept the default value or enter a new value at each prompts.

> **ATTENTION**
> You must know the root password to perform the following procedure.

Procedure 1
Installing the MCG 3100 software

Step	Action
1	At the server (host server), insert the MCG 3100 software CD into the CD-ROM drive.
2	Log on to the server as nortel. For more information, see "Admin shell access" (page 50).

3. Locate the MCG 3100 software on the CD and enter the following command:

   ```
   appinstall
   ```

   The installation script prompts you for the root password.

4. Enter the root password.

   The following prompt appears:

   ```
   Do you want to check the media [Y][N]?
   ```

5. To verify the media, enter **Y** (Yes).

   For a new installation, the following prompt appears:

   ```
   Installation stage Nortel MCG 3100 Mobile Gateway
   Installation 1.  MCG 3100 5.00.20
   Please select the supported configuration # to
   install.
   ```

   For a software reinstallation, you receive a prompt to remove any previous installations.

6. To start a new installation, enter **1** and proceed to Step 8.

   OR

   To start a software reinstallation, select **Y** (Yes) to confirm the deletion, and proceed to Step 7.

7. If you receive a prompt to perform a reinstall (1) or an upgrade (2), enter **1** for a reinstall.

   The application RPM files are installed in the /opt/mobilitybase directory.

8. Read the Nortel software license agreement.

   ```
   NORTEL SOFTWARE LICENSE - IMPORTANT NOTICE:
   Carefully read this license agreement ("License")
   BEFORE (a) downloading this software ("Software"),
   (b) installing, using or accessing the software
   provided (also "Software"), or (c) installing or
   using the hardware unit provided with pre-enabled
   software (also "Software") or using or accessing
   such Software.
   ...
   ...
   ...
   Do you agree to the above license terms?  [yes or no]
   ```

9. To agree to the license agreement, enter**YES**

   The software installation proceeds.

   ```
   Nortel Mobile Communications Gateway 3100
   installation in progress
   ...
   ...
   ```

```
...
RPM installation complete.  Please follow post
installation instructions.
```

The term postinstallation instructions refers to the postinstallation configuration procedures. For more information, see "Postinstallation" (page 27).

10 Remove the CD.

11 Proceed to postinstallation configuration.

OR

For a redundant server implementation, repeat Step 1 to Step 10 on the second server.

--End--

Postinstallation

This chapter contains the following topics:

- "Overview " (page 27)
- "MCG 3100 Web Console logon" (page 27)
- "MCG 3100 parameter configuration" (page 28)
- "License file" (page 31)
- "Manage TLS certificates" (page 33)

After the MCG 3100 installation completes, the client software must be installed on the devices. For instructions on installing the client software, see *Nortel Mobile Communication Gateway 3100 — Administration (NN42030-600)*.

Overview

Before you can use the Nortel Mobile Communication Gateway 3100 (MCG 3100) server to provide IP telephony services, you must perform the following postinstallation tasks:

- "MCG 3100 Web Console logon" (page 27)
- "MCG 3100 parameter configuration" (page 28)
- "License file" (page 31)
- "Manage TLS certificates" (page 33)

MCG 3100 Web Console logon

You must log on to the Web Console to configure the MCG 3100 parameters and to add the license file.

Procedure 2
Logging on to the MCG 3100 Web Console

Step	Action

1	In a Web browser address bar, enter one of the following addresses:
	`http://<hostname>:8282/adminserver`
	OR
	`https://<hostname>:8553/adminserver/`
	where
	`<hostname>` `is the domain name of the server.`

2	At the Web Console log on screen, enter the following default username and password: • Username: admin • Password: password The username and password are case sensitive. **ATTENTION** Nortel recommends that you change the default password.
3	Click **Sign In**.

--End--

MCG 3100 parameter configuration

You must configure the MCG 3100 parameters to communicate with the following network elements:

- Enterprise Communications Server (ECS)
- Backup MCG 3100 (if installed)
- Lightweight Directory Access Protocol (LDAP) Server

Use the Configuration window buttons for the following tasks:

- **Unlock**—unlocks the configuration parameters to enable them to be updated.
- **Lock**—locks the configuration parameter fields.
- **Save**—saves updates and prompts you to restart the server.
- **Load current values**—restores the current server values to the parameter fields.

Procedure 3
Configuring the MCG 3100 parameters

Step	Action
1	Log on to the MCG 3100 Web Console using the Administrator username and password, as described in Procedure 2 “Logging on to the MCG 3100 Web Console” (page 27).
2	Click **Gateway**.
3	Click **Configuration** for the Gateway you want to modify.
4	Click **Unlock**. The configuration parameters unlock and can be modified.
5	Modify the configuration parameters as required. For a description of the parameter fields, see Table 4 "MCG 3100 configuration parameter fields" (page 29).
6	Click **Save** to save the modified parameters.
7	Click **OK** to restart the server.

--End--

Table 4
MCG 3100 configuration parameter fields

Field	Description
Gateway Address	The IP address that the local MCG 3100 uses for HTTP traffic.
Backup Gateway SIP Listening Address	The IP address and port of the second MCG 3100 in a redundant pair. Syntax: [IP]:[port] Example: 192.167.130.76:5060
Gateway SIP Listening Address	The host name or IP address where the SIP gateway receives inbound SIP requests over UDP. Syntax: [IP]:[port] Example: 192.167.130.75:5060
Primary ECS Address	The IP address and port of the primary Enterprise Communication Server. For CS 1000, this is the primary SIP Proxy Server (SPS). Syntax: [IP]:[port] Example: 192.167.101.2:5060
Secondary ECS Address	The IP address and port of the secondary Enterprise Communication Server (if available). Syntax: [IP]:[port] Example: 192.167.101.2:5060
Group Call Server Address	The IP address and port of the group call server. The group call server IP address is the local MCG 3100 IP address with the port configured on the group call server page. Syntax: [IP]:[port] Example: 192.167.130.75:5072

Table 4
MCG 3100 configuration parameter fields (cont'd.)

Field	Description
LDAP Server Address	The IP address and port of the LDAP server that hosts the corporate directory. Obtain this value from the directory administrator. Syntax: [IP]:[port] Example: 192.167.3.99:389
LDAP Username	The username required to gain access to the LDAP server that hosts the corporate directory. Syntax: domain\username
LDAP Password	The password required to gain access to the LDAP server that hosts the corporate directory.
LDAP Search Base	The unique name of the search base object (node) that defines the location in the directory from which the LDAP search begins.
LDAP Security Authorization	The authorization mechanism used to connect to the LDAP server. The options are: • None (no authentication, anonymous) • Simple (usernames and passwords sent as clear text) The default value is simple.
Mobile Number Prefix	When Mobile Users accept an incoming call notification, they can choose where to take the call. They can take the call on their cell phone, home phone, an office extension, or on any of the preconfigured contact numbers on the MCC 3100. If the chosen number begins with the Mobile Number Prefix (usually a +), the caller hears a call progress announcement. If the chosen number does not have the prefix, the caller does not hear a progress announcement.
Gateway name	The gateway ID for the MCG 3100 that is defined on the communication server. For CS 1000, this is the gateway endpoint name for the MCG 3100 configured on the SPS.
User Prefix for Call Termination	The mobility Home Location Code (HLOC) that is added to the Personal Call Assistant (PCA) target Directory Number (DN) on the CS 1000 to ensure a uniquely routable number from the PCA to the MCG 3100. The MCG 3100 uses this parameter to strip leading digits from the request-URI to produce the username of the MCC 3100 for which the call is destined.
User Prefix/Phone-context for Call Origination	The parameter applied to the p-asserted-id (PAI) as input to the Sourced-based routing (SBR) feature on the CS 1000 SPS. If the input is a digit the digit is prepended to the username portion of the PAI. If the input is not a digit, a phone-context=<input> parameter is added.

Table 4
MCG 3100 configuration parameter fields (cont'd.)

Field	Description
Dial In Service DN	This is the number in the request URI for service DN calls proxied by the CS 1000 SPS to the MCG 3100. The service DN allows MCG 3100 users to place calls directly from their wireless devices to other parties using Direct Outbound call mode.
Enterprise numbers are directly dialable	This parameter is permanently enabled on the MCG 3100
Domain	The realm for SIP registration defined on the Enterprise Communication Server.

License file

The license file controls how many MCC 3100 users can log on to the MCG 3100. For example, if your organization purchased a 100-seat license, a maximum of 100 users can be licensed and log on.

ATTENTION
Licenses are allocated on a first-come, first-served basis, and they remain allocated until the Administrator deallocates them.

The Administrator must obtain the license file from Nortel and install it on the MCG 3100 Server. For more information, see Procedure 4 "Adding a license file" (page 31).

Procedure 4
Adding a license file

Step	Action
1	Obtain the license file and store it in a location that is accessible from the MCG 3100 Server.
2	Log on to the MCG 3100 Web Console as an administrative user.
3	Select the **Tools** tab.
4	On the **Tools** page, under **License Upgrade**, click **Browse**.
5	In the **Choose file** dialog, locate and select the license file to upload, and then click **Open**.
6	Click **Upload**.
7	Select the **Gateway** tab.
8	Click **Restart**.

9 For a redundant server implementation, repeat Step 2 to Step 8 on the redundant server.

--End--

Licence file troubleshooting

Before you contact Nortel to report a licensing issue, perform the following troubleshooting measures:

- Check the time, date, and time zone of the server.
- Check the route to the license server (ping).
- Verify DNS for the license server.
- Check error diagnostics on Gateway Configuration page.
- Restart the MCG 3100 server.

> **ATTENTION**
> Always restart the MCG 3100 server after you provide a valid license file or perform any changes to solve any licensing issue.

Table 5 "Common server license status errors" (page 32) lists some of the most common server license status errors that can occur.

Table 5
Common server license status errors

Server License Status	Issue description	Resolution
License file not found	The license file is not uploaded.	Upload a valid license file and restart.
License is invalid	This error indicates that the license file is already activated on another server.	Upload a valid license file and restart.
License expired	This error indicates that the license file is already activated on another server.	Upload a valid license file and restart.
ERROR 23: protocol violation	This error indicates that the local system clock is out of sync with the time on the licensing server.	Reset the system clock and restart.

Table 5
Common server license status errors (cont'd.)

Server License Status	Issue description	Resolution
ERROR 103: Client's system clock is suspect and/or the client configuration has been tampered with.	This error indicates that the system clock was changed after a previous activation.	Reset the system clock and restart.
ERROR 17: key limit exceeded	This error indicates that the license file that you provided was activated before on another machine and there is no seat available for you to activate.	Contact Nortel.

> **ATTENTION**
> If you start the MCG 3100 for the very first time without a valid license, errors occur until you upload a valid license and restart the server. You must always restart the MCG 3100 after you add or modify the license file.

Manage TLS certificates

A Public Key Infrastructure (PKI) uses Transport Layer Security (TLS) certificates to provide server authentication and private communication. With a PKI, the communication between the mobile clients and the MCG 3100 server is secure.

Perform the following tasks to configure the PKI:

- Enroll with a Certificate Authority (CA).
- Generate a Certificate Signing Request (CSR).
- Obtain a signed TLS certificate.
- Obtain the CA root certificate, intermediate certificate, or both as required by the CA..
- Install the root or intermediate (or both as required by the CA) and signed certificates.
- Distribute the CA root certificate.

Enroll with a Certificate Authority

Some CAs, such as VeriSign or Entrust, charge a fee for their services. Others, such as CACert or RapidSSL, provide free or low-cost solutions. As an alternative to using a commercial CA, you can build your own. For example, Microsoft Exchange Server includes tools that enable you to build a CA server that is exclusive to your organization.

Whether you select a commercial Certificate Authority (CA) or build your own CA Server, you must provide the following information to enroll:

- first and last name of the certificate administrator
- e-mail address of the certificate administrator
- any other information requested by the CA

ATTENTION
Nortel strongly recommends that you create an e-mail alias for the certificate administrator. The CA sends renewal notifications and other important information to this e-mail address. If the administrative responsibilities are shared, any administrator can access the notifications.

For additional information about commercial Certificate Authorities, go to any one of the following company Web sites:

- VeriSign
- Entrust
- CACert
- RapidSSL

For additional information about building your own CA server with Microsoft Exchange Server 2007, go to the Microsoft Web site at http://www.microsoft.com. Search on the key words *build a certificate authority*.

Certificate Signing Request generation

A Certificate Signing Request (CSR) is the unique fingerprint of the server and includes your private and public key pair. You need a CSR to enroll for a TLS certificate.

Procedure 5 “Generating a CSR” (page 35) describes the steps to generate a CSR by using Java keytool and sample directories. In this procedure, you use Java keytool, which is the recommended method. You can use another tool to generate a CSR if your environment requires that you do so.

For more information about Java keytool, go to http://java.sun.com/ and search on the keyword *keytool*.

A keystore is a file that can contain trusted certificates and combinations of private keys with their corresponding certificates. The information within the keystore is organized by alias, for example:

- tomcat (required): stores the public/private key pair and the Signed TLS Certificate from the CA
- root (required): stores the CA root certificate information
- intermediate (required for some CAs): stores the CA intermediate certificate information

Procedure 5
Generating a CSR

Step	Action
1	At the MCG 3100 Server, log on to the server as nortel.
2	To become the superuser, enter the following command: **`su`**
3	To change to the certificate keystore directory, enter: **`cd /opt/SQMobilityGW`**
4	To delete the default keystore, enter: **`rm .keystore`**
5	To generate a certificate keystore and private key, enter: **`/usr/java/jdk1.5.0_03/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore .keystore`**
6	At the prompt, enter the password for the keystore: **`firsthand`** The default password for the keystore is firsthand. If you want to change the default password, you must modify the .xml configuration file for the MCG 3100 Server. For more information, see "Change the keystore default password" (page 40).
7	Enter the following information as required by the CA: • First and last name—the Common Name of the keystore. Use the host name (including domain name) of the server as the common name (cn). For example: mg.mydomain.com

> **ATTENTION**
> For the mobile clients that use TLS security, you must enter the same FQDN in the device System Settings. For information about the configuration of the System Settings on the device, see *Nortel Mobile Communication Client 3100 for Blackberry User Guide (NN42030-101)* , *Nortel Mobile Communication Client 3100 for Nokia User Guide (NN42030-102)* and *Nortel Mobile Communication Client 3100 for Windows Mobile Single Mode User Guide (NN42030-107)*.

- Organization—your company or organization’s formal name
- Organizational unit—the department, division or other organizational unit that will use this certificate
- City/Location—the city in which your organization is located
- State/Province—the state or province in which your organization is located
- Country—the country in which your organization is located

Example

```
What is your first and last name?
[Unknown]: mcg3100.nortel.com
What is the name of your organizational unit?
[Unknown]: Tech Trials
What is the name of your organization?
[Unknown]: Nortel networks
What is the name of your City or Locality?
[Unknown]: Belleville
What is the name of your State or Province?
[Unknown]: Ontario
What is the two-letter country code for this
unit?
[Unknown]: CA
```

8 At the prompt, enter the key password for <tomcat>.

OR

If the password is the same as the keystore password, press **Enter**.

9 To change ownership of the keystore from root to mobility, enter:

```
chown nortel:nortel .keystore
chmod 755 .keystore
```

10 To generate the CSR, enter:

```
/usr/java/jdk1.5.0_03/bin/keytool -certreq
-alias tomcat -keystore .keystore
```

11 Enter the keystore password:

`firsthand`

The CSR text appears as in the following example:

Sample CSR text

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBJTCB0AIBADBtMQswCQYDVQQGEwJVUzEQMA4G
A1UEChs4lBMHQ XJpem9uYTENA1UEBxMETWVzYTEf
MB0GA1UEChMWTWVs3XbnzYSBDb 21tdW5pdHkgQ2
9sbGVnZTEA1UEAxMTd3d3Lm1jLm1hcmljb3BhLmV
kdTBaMA0GCSqGSIb3DQEBAQUAA0kAMEYCQQDRNU6
xslWjG41163gA rsj/P108sFmjkjzMuUUFYbmtZX4
RFxf/U7cZZdMagz4IMmY0F9cdp DLTAutULTsZKD
cLAgEDoAAwDQYJKoZIhvcNAQEEBQADQQAjIFpTLg
fmBVhc9SQaip5SFNXtzAmhYzvJkt5JJ4X2r7VJYG3J
0vauJ5VkjXz 9aevJ8dzx37ir3P4XpZ+NFxK1R=
-----END NEW CERTIFICATE REQUEST-----
```

12 Copy the entire CSR text, including `-----BEGIN NEW CERTIFICATE REQUEST-----` and `-----END NEW CERTIFICATE REQUEST-----` and save it as a text file, for example CSR.txt.

13 Store the CSR text file in a safe location.

You require the CSR text file to request a signed TLS certificate from the CA.

--End--

Signed TLS certificate

You must obtain a signed TLS certificate from the CA and install it in your keystore. To obtain the signed TLS certificate from the CA, follow the steps in Procedure 6 “Obtaining a signed TLS certificate” (page 37). Before you begin, ensure that you have access to the CSR file that you saved in Procedure 5 “Generating a CSR” (page 35) Step 12.

Procedure 6
Obtaining a signed TLS certificate

Step Action

1 Using the certificate management tool provided by your CA, access the prompt or Web page where you request certificates.

2 If you receive a prompt to specify the server type, select **Apache**.

3 At the prompt or Web page, paste the entire CSR text, including `-----BEGIN NEW CERTIFICATE REQUEST-----` and `-----END NEW CERTIFICATE REQUEST-----`.

OR

Upload the CSR.txt file.

4 Request a signed TLS certificate.

The CA generates a signed TLS certificate and sends it to the certificate administrator’s e-mail address.

5 Save the signed TLS certificate to a location that is accessible from the MCG 3100 Server.

You require the signed TLS certificate to perform “Root and signed certificate installation” (page 39) Step 5.

--End--

CA root and intermediate certificates

You must obtain the CA root or intermediate certificate in two formats:

- TXT format for installation on the server
- DER format for installation on the mobile devices

To obtain the CA root or intermediate certificate, use the certificate management tool provided by the CA and follow the steps in Procedure 7 “Obtaining a CA root or intermediate certificate” (page 38).

> **ATTENTION**
> In some cases the CA provides an intermediate certificate instead of, or in addition to, the root certificate. Read all instructions provided by the CA carefully. Follow the same procedure to download an intermediate certificate, as for the root certificate.

Procedure 7
Obtaining a CA root or intermediate certificate

Step	Action
1	Using the certificate management tool provided by your CA, locate the root or intermediate certificate in both TXT and DER formats.
2	Download the TXT format for the server. You can skip this step if your server is preconfigured with your CA root certificate.
3	Download the DER format for the client devices. You can skip this step if the client devices are preconfigured with your CA root or intermediate certificate.

4 Save both formats of the certificate to a directory location that is accessible from the MCG 3100 Server.

--End--

Root and signed certificate installation

The keystore must contain the following certificates:

- the CA root or intermediate certificate (or both as required by the CA) in TXT format
- your signed TLS certificate

Procedure 8 “Installing the root and signed certificates” (page 39) describes the steps to import the certificates. You must know the root password to perform the following procedure. Root certificate files require Read and Write permissions for the user nortel.

> **ATTENTION**
> The root certificates for some well-known CAs (such as Verisign and Entrust) are preinstalled on the server and many client devices. If you receive a message stating that a certificate is already installed, select Yes to replace it, or No to use the existing certificate.

Procedure 8
Installing the root and signed certificates

Step **Action**

1 At the MCG 3100 Server, log on to the server as nortel.

2 Change to the certificate keystore directory:

```
cd /opt/SQMobilityGW
```

3 If the CA requires a root certificate, import it (in TXT format):

```
/usr/java/jdk1.5.0_03/bin/keytool -import
-trustcacerts -keystore .keystore -alias root
-file <absolute_path_root_certificate_file>
```

4 If the CA requires an intermediate certificate, import it (in TXT format):

```
/usr/java/jdk1.5.0_03/bin/keytool -import
-trustcacerts -keystore .keystore
-alias intermediate
-file <absolute_path_intermediate_cert_file>
```

5 Import the signed TLS certificate:

```
/usr/java/jdk1.5.0_03/bin/keytool -import
-trustcacerts -keystore .keystore -alias tomcat
-file <absolute_path_signed_certificate_file>
```

> **ATTENTION**
> Nortel strongly recommends that you back up the keystore directory to protect the files against overwriting, deletion, or corruption.

6 Restart the server:

```
/sbin/service mobilitygw restart
```

7 When prompted, enter the root password.

--End--

Importing a preinstalled CA root or intermediate certificate

You must know the absolute path to import a preinstalled CA root certificate into the keystore. Enter one of the following commands:

```
/usr/java/jdk1.5.0_03/bin/keytool -import
-trustcacerts -keystore .keystore -alias root
-file <absolute_path_root_certificate_file>
```

OR

```
/usr/java/jdk1.5.0_03/bin/keytool -import -trustcacerts
-keystore .keystore -alias intermediate -file
<absolute_path_intermediate_cert_file>
```

Viewing the contents of the keystore

To assist with troubleshooting, you can review the contents of the keystore. Enter the following command:

```
/usr/java/jdk1.5.0_03/bin/keytool -list -v -keystore
.keystore
```

Change the keystore default password

The default password for the keystore is firsthand. For security reasons, you should change the default password.

Procedure 9
Changing the keystore default password

Step	Action

1 At the MCG server, log on to the server as nortel.

2 To become the superuser, enter the following command:
```
su
```

3 To change the keystore default password, enter the following command:

```
/usr/java/jdk1.5.0_03/bin/keytool -storepasswd
-new <new_password> -storepass <od_password>
-keystore /opt/SQMobilityGW
```

where

<old_password> is the existing keystore password.
<new_password> is your chosen password.

4 Change the working directory:

```
cd /opt/SQmobilityGW/tomcat/conf/
```

5 Open the server.xml file using an available editor (for example, vi).

6 Locate the following default line:

```
clientAuth="false" sslProtocol="TLS" key
storeFile="/opt/SQMobilityGW/.keystore"
keypass="firsthand"
```

7 Change `keypass="firsthand"` to `keypass="<new_password>"`.

where

<new_password> is the password entered in the `keytool` command.

8 Save and close the server.xml file.

9 Restart the service:

```
sudo /sbin/service mobilitygw restart
```

--End--

CA root certificate distribution

You must ensure the CA root certificate is installed (in DER format) on all mobile client devices that register with the MCG 3100 Server. Depending on which CA you choose, the root certificates are preinstalled or you distribute the root certificates to the clients for manual installation.

Various methods of root certificate distribution are available. Typically, the administrator e-mails the root certificate to the mobile client users who need it (Windows Mobile Single Mode and Nokia clients). The users must install the certificate on their devices.

After the user installs the root certificate, the mobile client communicates with the MCG 3100 using TLS security.

ATTENTION
If a user attempts to log on and the root certificate is not installed, a prompt appears asking for permission to allow access to the MCG 3100 Server. If permission is granted and the connection fails or times out, the user must install the root certificate on the mobile client device.

When you send the root certificate to the users, you should send the following procedures in the e-mail.

Procedure 10
Installing a root certificate on a Nokia device

Step	Action
1	On the PC, open the Nokia PC Suite by choosing **Start > Programs > Nokia PC Suite > Nokia PC Suite**.
2	Click **File Manager**.
3	In the Nokia Phone Browser, browse to the folder that contains the root certificate, and then select and copy the root certificate.
4	Paste the root certificate into the **Nokia Phone Browser > Nokia <E6x> > Phone memory > Data > Documents** folder.
5	On the Nokia phone, press the **Menu** key.
6	On the Menu screen, select **Office > File mgr > Documents**.
7	In the Documents folder, select the certificate.
8	Select **Options > Open**. You receive a prompt to save the certificate and a security warning appears.
9	Click **Yes**.
10	Specify a label for the certificate and click **OK**.
11	After the **Certificate Uses** prompt appears, select Internet. The root certificate installs in the Tools > Settings > Security > Certif. Management directory.

--End--

Procedure 11
Installing a root certificate on a Windows Mobile Single Mode device

Step	Action
1	On the PC, connect the mobile device using a USB cable.
2	On the PC, start the ActiveSync program, and click **Explore**.
3	Copy the root certificate file (a .cer file) to the device.

4 On the device, locate the certificate using File Explorer and click on it.

5 At the continuation prompt , click **Accept**.

The certificate installs on the device.

--End--

System software maintenance

This chapter contains the following topics:

System software upgrades

After you complete the initial Mobile Communication Gateway (MCG) 3100 system software installation (a fresh install), you can upgrade the system software.

You can upgrade the system using

- an MC 3100 software CD
  For more information, see Procedure 12 “Upgrading the MCG 3100 system software from CD” (page 45).
- a software Service Update (SU) or patch downloaded from the Web
  For more information, see Procedure 13 “Upgrading the MCG 3100 system software from the Web” (page 46).

You can also remove an SU. For more information, see Procedure 14 “Removing an SU” (page 48).

ATTENTION
If you have previously installed an SU, you must remove it before installing a new SU. For more information, see Procedure 14 “Removing an SU” (page 48)

Procedure 12
Upgrading the MCG 3100 system software from CD

ATTENTION
You must know the root password to perform the following procedure.

Step	Action
1	At the server (host server), insert the MCG 3100 software CD into the CD-ROM drive.
2	Log on to the server as nortel.
3	Locate the MCG 3100 software on the CD and run the following command: `appinstall`
4	Enter the root password.
5	If you are prompted to remove a previous installation, enter **Y** (Yes) to confirm the deletion.
6	If you are prompted to perform a reinstall (1) or an upgrade (2), press Enter to accept the default value (2). The application RPM files are installed in the /opt/mobilitybase directory.
7	Read the Nortel software license agreement.
8	To agree to the license agreement, enter **YES**
9	For a redundant server implementation, repeat Step 1 to Step 8 on the second server.

--End--

Procedure 13
Upgrading the MCG 3100 system software from the Web

> **ATTENTION**
> You must have access to the Nortel Enterprise Solutions PEP Library (ESPL) and you must know the MCG 3100 root password to perform the following procedure.

> **ATTENTION**
> If you have previously installed an SU, you must remove it before installing a new SU. For more information, see Procedure 14 “Removing an SU” (page 48)

Step	Action
1	From an internet-connected computer, connect to http://www.nortel.com/espl.
2	After logging in, read the warning and then click **Click Here**.
3	Scroll to the Communication Server 1000 / Meridan 1 PEP Tools section, locate the Patching Reference for CS 1000 Release 5.0 Systems, and click **Click Here** beside the entry.

The document contains information about SUs for CS 1000.

4 Download the appropriate patches to a location that you can connect to from the MCG 3100.

5 Log on to the MCG 3100 as nortel.

For more information, see "Admin shell access" (page 50).

6 Transfer the SU you downloaded to the /var/opt/nortel/patch directory of the MCG 3100.

> **ATTENTION**
> The patching software requires all patch files to be stored in the /var/opt/nortel/patch directory.

7 Access the MCG 3100 command line.

8 To view the current version of software, enter **`swVersionShow`**

The MCG 3100 responds with the current version of the software, for example:

```
Configuration installed:  MCG3100
Configuration version:  5.00.20
mobilitybase 2.1-48
nortel-cs1000-linuxbase 5.00.38
```

9 To install the load, enter **`pload`**

10 When the program prompts `Patch filename?`, enter the patch filename.

The MCG 3100 installs the SU, and reports on the success of the installation. For example:

```
Patch filename?mobilitybase-2.1.75.el4
Patch mobilitybase-2.1.75.el4
Patch successfully installed.
```

11 To put the SU in service, enter **`pins 0`**

The MCG 3100 responds:

```
Patch handle:  0
The application mobilitybase should be stopped
before putting in service this Service Update
Do you want to continue?  (Y/N) [N]?
```

12 Enter **`y`**

The installation continues, displaying its progress. For example:

```
Performing the installation:
Name :  mobilitybase Relocations:  (not
relocatable)
Version :  2.1 Vendor:  (none)
Release :  75 Build Date:  Thu 14 Feb 2008 12:53:03
PM EST
Install Date:  (not installed) Build Host:
masterserver.sipquest.com
Group Applications/Communications Source RPM:
```

```
mobilitybase-2.1-75.src.rpm
Size :  72043134 License:  Commercial Signature :
(none)
Summary :  Mobility Gateway Base distribution
package
Description :
facility for the configuration of the platform for
the mobility gw
```

The server completes the installation.

13 Enter
`sudo /opt/mobilitybase-2.1-XX/postpatch.sh`

where

XX is the load number being installed.

The server completes the installation, which ends with the message `Post patch complete`.

14 To check the SU installation, enter **`pstat`**

The server responds with information about the SU status. For example,

```
In system patches:1
Patch handle 0*
Filename /var/opt/nortel/patch/mobilitybase-2.1.
75.el4
Patch release version:  5.00.38
Reference number:  ISS1:1OF1
Patch is in-service
In-service date:  14/02/08 15:15:46
Patch category:  GEN
Patch special instructions:  no
Patch member type:  RPM
Patch members:  mobilitybase-2.1-75.i386.rpm
```

15 Verify that the version of the SU displays in the server response.

--End--

If you need to remove an SU, use the following procedure.

Procedure 14
Removing an SU

Step	Action
1	Log on to the MCG 3100 as nortel. For more information, see “Admin shell access” (page 50).
2	To list the current patches and SUs in service, enter **`pstat`**

The server responds with information about the SU status. For example,

```
In system patches:1
Patch handle 0*
Filename /var/opt/nortel/patch/mobilitybase-2.1.
75.el4
Patch release version:  5.00.38
Reference number:  ISS1:1OF1
Patch is in-service
In-service date:  14/02/08 15:15:46
Patch category:  GEN
Patch special instructions:  no
Patch member type:  RPM
Patch members:  mobilitybase-2.1-75.i386.rpm
```

3 To take a patch or SU out of service, enter **`poos 0`**

The server responds

```
Patch handle: 0
The application mobilitybase should be stopped before putting
out of service this Service Update
Do you want to continue? (Y/N) [N]?
```

4 Enter y

The RPM patch removal completes.

5 To complete the removal, enter
`sudo /opt/mobilitybase-2.1-XX/postunpatch.sh`

where

`XX` `is the load number being removed.`

The server continues the removal, which ends with the message

```
Pre uninstall phase done.
Post uninstall phase done.
Updating iptables rules:  [ OK ].
```

6 To verify that the SU was removed correctly, enter
`swVersionShow`

The server responds with the version. For example,

```
Configuration installed:  MCG3100
Configuration version:  5.00.20
mobilitybase 2.1-48
nortel-cs1000-linuxbase 5.00.38
```

--End--

System software uninstallation

You uninstall the Nortel Mobile Communication Gateway 3100 (MCG 3100) system software from the command line.

Procedure 15
Uninstalling the MCG 3100 system software

> **WARNING**
> This procedure removes the MCG 3100 software from the server. Use Procedure 14 “Removing an SU” (page 48) to remove patches.

Step **Action**

1 Log on to the server as nortel.

2 From any directory, enter the uninstall command:

```
sudo rpm -e mobilitygw mobilityadmin sq-base
sq-conf mobileclients
```

--End--

Admin shell access

Many of the maintenance procedures require that you access the admin shell and log on using the nortel user account. You have two options for admin shell access:

- serial port connection
- Secure Shell (SSH)

For more information about accessing the admin shell, see *Linux Platform Base and Applications Installation and Commissioning (NN43001-315).*

Shell commands

You can use Linux shell commands to perform the following tasks:

- Start, stop, or restart the server processes
- Check whether the server processes are running
- Back up and restore the server databases

For more information, see the following procedures:

- Procedure 16 “Starting, stopping, and restarting the MCG 3100 Server” (page 51)
- Procedure 17 “Starting, stopping, and restarting the Administration Server” (page 51)
- Procedure 18 “Starting, stopping, and restarting the Group Call Server” (page 51)

- Procedure 19 “Checking the Gateway Server processes” (page 52)
- Procedure 20 “Checking the Administration Server processes” (page 53)
- Procedure 21 “Backing up the databases” (page 54)
- Procedure 22 “Restoring the databases” (page 54)

Procedure 16
Starting, stopping, and restarting the MCG 3100 Server

Step	Action
1	Log on to the server as nortel.
2	To start the MCG 3100, enter `sudo /sbin/service mobilitygw start`
3	To stop the MCG 3100, enter `sudo /sbin/service mobilitygw stop`
4	To restart the MC 3100, enter `sudo /sbin/service mobilitygw restart`

--End--

Procedure 17
Starting, stopping, and restarting the Administration Server

Step	Action
1	Log on to the server as nortel.
2	To start the Administration server, enter `sudo /sbin/service mobilityadmin start`
3	To stop the Administration server, enter `sudo /sbin/service mobilityadmin stop`
4	To restart the Administration server, enter `sudo /sbin/service mobilityadmin restart`

--End--

Procedure 18
Starting, stopping, and restarting the Group Call Server

Step	Action
1	Log on to the server as nortel.

2 To start the Group Call Server, enter

```
sudo /sbin/service sipconf start
```

3 To stop the Group Call Server, enter

```
sudo /sbin/service sipconf stop
```

4 To restart the Group Call Server, enter

```
sudo /sbin/service sipconf restart
```

--End--

Procedure 19
Checking the Gateway Server processes

Step **Action**

1 Log on to the server as nortel.

For more information, see "Admin shell access" (page 50).

2 At the command prompt, enter the following command:

```
ps -ef | grep SQMobilityGW
```

The following sample output indicates that the process is running. If only one line appears, the process is stopped and you must use the restart the procedure. For more information, see Procedure 16 "Starting, stopping, and restarting the MCG 3100 Server" (page 51).

```
mobility 2400 1 0 Jun12 ?  00:22:22
/usr/java/jdk1.5.0_03/bin/java -Xmx512m -Dcom
.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.port=9800
-Dcom.sun.management.jmxremote.ssl=false -Djava.
util.logging.manager=org.apache.juli.ClassLoader
LogManager -Djava.util.logging.config.file=/opt/
SQMobilityGW/tomcat/conf/logging.properties
-Djava.endorsed.dirs=/opt/SQMobilityGW/tom
cat/common/endorsed -classpath :/opt/SQMobi
lityGW/tomcat/bin/bootstrap.jar:/opt/SQMob
ilityGW/tomcat/bin/commons-logging-api.jar
-Dcatalina.base=/opt/SQMobilityGW/tomcat
-Dcatalina.home=/opt/SQMobilityGW/tomcat
-Djava.io.tmpdir=/opt/SQMobilityGW/tomcat/temp
org.apache.catalina.startup.Bootstrap start

root 9498 9367 0 14:02 pts/0 00:00:00 grep
SQMobilityGW
```

If the process is not running, only the following line appears:

```
root 9498 9367 0 14:02 pts/0 00:00:00 grep
SQMobilityGW
```

--End--

Procedure 20
Checking the Administration Server processes

Step	Action
1	Log on to the server as nortel. For more information, see “Admin shell access” (page 50).
2	At the command prompt, enter the following command:

```
ps -ef | grep SQMobilityAdmin
```

The following sample output indicates that the process is running. If only one line appears, the process is stopped and you must use the restart the procedure. For more information, see Procedure 17 “Starting, stopping, and restarting the Administration Server” (page 51).

```
root 2374 1 0 Jun12 ?  00:50:10
/usr/java/jdk1.5.0_03/bin/java -Xmx512m -Dcom
.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.port=9801
-Dcom.sun.management.jmxremote.ssl=false -Djava.
util.logging.manager=org.apache.juli.ClassLoader
LogManager -Djava.util.logging.config.file=/opt
/SQMobilityAdmin/tomcat/conf/logging.properties
-Djava.endorsed.dirs=/opt/SQMobilityAdmin/tom
cat/common/endorsed -classpath :/opt/SQMobili
tyAdmin/tomcat/bin/bootstrap.jar:/opt/SQMobi
lityAdmin/tomcat/bin/commons-logging-api.jar
-Dcatalina.base=/opt/SQMobilityAdmin/tomcat
-Dcatalina.home=/opt/SQMobilityAdmin/tomcat -Dj
ava.io.tmpdir=/opt/SQMobilityAdmin/tomcat/temp
org.apache.catalina.startup.Bootstrap start
root 9542 9367 0 14:04 pts/0 00:00:00 grep
SQMobilityAdmin
```

If the process is not running, only the following line appears:

```
root 9542 9367 0 14:04 pts/0 00:00:00 grep
SQMobilityAdmin
```

--End--

CAUTION
Service Interruption
The database backup and restore procedures take the server out of service for two or more minutes. Nortel recommends that you perform these procedures during periods of low server use.

The database stores configuration data and licensed user data. You must know the root password to perform the database backup and restore procedures.

Procedure 21
Backing up the databases

Step **Action**

1 Log on to the server as nortel.

2 To become the root user, enter

su - root

3 Enter the password for root.

4 Stop the server processes by entering

```
/sbin/service sipconf stop
/sbin/service mobilitygw stop
/sbin/service mobilityadmin stop
```

5 Create a backup directory:

```
mkdir /opt/backup
```

6 Change to the backup directory:

```
cd /opt/backup
```

7 At the command prompt, enter:

```
mysqldump --opt --all-databases >backup.sql
```

8 Copy the backup file to an off-site location or removable media.

9 Start the server processes:

```
/sbin/service sipconf start
/sbin/service mobilitygw start
/sbin/service mobilityadmin start
```

--End--

Procedure 22
Restoring the databases

ATTENTION
You must have a copy of the backup file to restore.

Shared files for group calls and conferences are not restored with this procedure.

Step	Action
1	Log on to the server as nortel.
2	To become the root user, enter su - root
3	Enter the password for root.

4	To stop the server processes, enter
	`/sbin/service sipconf stop`
	`/sbin/service mobilitygw stop`
	`/sbin/service mobilityadmin stop`

5	To change to the backup directory, enter **`cd /opt/backup`**
6	Copy the backup file from the off-site location or removable media to the backup directory.

7	Enter the following commands:
	`mysql <backup.sql`
	`mysqladmin flush-privileges`

8	To start the server processes, enter
	`/sbin/service sipconf start`
	`/sbin/service mobilitygw start`
	`/sbin/service mobilityadmin start`

--End--

Appendix A
Port numbers and protocols

Table 6 "Port usage" (page 57) lists the port usage details for the MCG 3100.

Table 6
Port usage

Port	Protocol	Function	Application	Configurable	Port mapped through firewall
21	TCP	FTP	Base Linux	No	No
22	TCP	SSH	Base Linux	No	No
53	UDP	Domain Name Server (DNS) queries to external DNS	MCG 3100	No	No
123	TCP	NTP	Base Linux	No	No
3306	TCP	SQL Client access	MySQL	No	No
5060	UDP	MCG 3100 SIP interface	MCG 3100	Yes	No
5072	UDP TCP	MCG 3100 Group Call SIP interface	MCG 3100	Yes	No
7800	TCP	MCG 3100 data replication	MCG 3100	No	No
8080	TCP	MCG 3100 Client interface	MCG 3100 Gateway	No	No

Table 6
Port usage (cont'd.)

Port	Protocol	Function	Application	Configurable	Port mapped through firewall
8282	TCP	MCG 3100 Admin interface	MCG 3100 Admin	No	No
8443	TCP	MCG 3100 Secure Client interface	MCG 3100 Gateway	No	No
8553	TCP	MCG 3100 Secure Admin interface	MCG 3100 Administration	No	No
9800	TCP	JVM Management interface	MCG 3100 Gateway JVM	No	No
9801	TCP	JVM Management interface	MCG 3100 Administration JVM	No	No
26 000 – 26 999	UDP	RTP Stream port range	MCG 3100 Group Call	Yes	No

Appendix B
Self-signed certificate generation

As an alternative to using a Certificate Authority, you can generate and use self-signed certificates.

ATTENTION
Self-signed certificates do not provide the same level of security as CA-signed certificates. Use self-signed certificates for test or demonstration purposes only.

For more information about the Java keytool, go to http://java.sun.com/ an d search on the keyword *keytool*.

Procedure 23
Generating self-signed certificates

Step	Action
1	Log on to the server as nortel.
2	To become the superuser, enter the following command: **su**
3	Change to the certificate keystore directory: **cd /opt/SQMobilityGW/**
4	Delete the default keystore: **rm .keystore**
5	Generate a self-signed certificate keystore and certificate: **/usr/java/jdk1.5.0_03/bin/keytool -genkey -alias Tomcat -keyalg RSA -storepass firsthand -keypass firsthand -dname 'cn=<common name>' -keystore .keystore -validity xxx** where **xxx** represents the number of days until the certificate expires. The default value is

```
90 days.  Nortel recommends using a value of
3650.
```

ATTENTION
Use the host name (including domain name) of the server as the common name (cn).

6 Generate the client certificate:

```
/usr/java/jdk1.5.0_03/bin/keytool -export
-alias Tomcat -file publickey.der
-storepass firsthand -keypass firsthand
-keystore .keystore
```

7 Use a file management utility to move the client certificate to a location where it can be distributed to users.

8 Restart the server by entering

```
service mobilitygw restart
```

--End--

Index

Nortel Mobile Communication 3100 Series Portfolio

Nortel Mobile Communication Gateway 3100 Installation and Upgrades

Sourced in Canada
Release: 2.1
Publication: NN42030-300
Document status: Standard
Document revision: 02.03
Document release date: 9 May 2008

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

LEGAL NOTICE

This document contains Nortel confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without Nortel’s express written authorization. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.